ADDITIVE DECOMPOSITIONS OF SUBGROUPS OF FINITE FIELDS

IGOR E. SHPARLINSKI

Abstract. We say that a set $\mathcal{S}$ is additively decomposed into two sets $\mathcal{A}$ and $\mathcal{B}$, if $\mathcal{S} = \{a + b \ : \ a \in \mathcal{A},\ b \in \mathcal{B}\}$. Here we study additively decompositions of multiplicative subgroups of finite fields. In particular, we give some improvements and generalisations of results of C. Dartyge and A. Sárközy on additive decompositions of quadratic residues and primitive roots modulo p. We use some new tools such the Karatsuba bound of double character sums and some results from additive combinatorics.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements. As usual, for two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ we define their sum as

$$\mathcal{A} + \mathcal{B} = \{a + b \ : \ a \in \mathcal{A},\ b \in \mathcal{B}\}.$$

We say that a set $\mathcal{S} \subseteq \mathbb{F}_q$ is *additively decomposed* into two sets if $\mathcal{S} = \mathcal{A} + \mathcal{B}$. We say that an additively decomposition is nontrivial if

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \ge 2.$$

Sárközy [17] has conjectured that the set $\mathcal{Q}$ of quadratic residues modulo a prime p does not have nontrivial decompositions and showed towards this conjecture that any nontrivial decomposition

$$\mathcal{Q} = \mathcal{A} + \mathcal{B}$$

satisfies

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \ge \frac{p^{1/2}}{3\log p} \qquad (1)$$

and

$$\max\{\#\mathcal{A}, \#\mathcal{B}\} \le p^{1/2}\log p \qquad (2)$$

2010 *Mathematics Subject Classification.* 11B13, 11L40.
Key words and phrases. Additive decompositions, finite fields, character sums, additive combinatorics.

Furthermore, Dartyge and Sárközy [6] have made a similar conjecture for the set $\mathcal{R}$ of primitive roots modulo p and given the following analogues of (1) and (2):

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \geq \frac{\varphi(p-1)}{\tau(p-1)p^{1/2}\log p} \tag{3}$$

and

$$\max\{\#\mathcal{A}, \#\mathcal{B}\} \leq \tau(p-1)p^{1/2}\log p \tag{4}$$

where $\varphi(k)$ and $\tau(k)$ are the Euler function and the number of integer positive divisors of an integer $k \geq 1$. We also refer to [6, 17] for further references about set decompositions.

Here we consider a more general question of additive decomposition of arbitrary multiplicative subgroups $\mathcal{G} \subseteq \mathbb{F}_q^*$. In particular, our results for large subgroups leads to improvements of the upper bounds (2) and (4), which in turn imply an improvement of the lower bounds (1) and (3). These improvements are based on an application of a bound of Karatsuba [14] of double multiplicative character sums. This technique work for subgroups of size or order at least $q^{1/2}$. For smaller subgroups in prime fields, that is, for prime $q = p$, we bring into this area yet another tool, coming from additive combinatorics. Namely, we use a result of Garaev and Shen [8]. We also use a result of Shkredov and Vyugin [19] on the size of the intetesection of shifts of a multiplicative subgroup, to obtain an upper bound on the cardinalities $\#\mathcal{A}$ and $\#\mathcal{B}$ for additive decomposition of arbitrary multiplicative subgroups $\mathcal{G} \subseteq \mathbb{F}_p^*$.

Finally, we note that Shkredov [18] has recently achieved remarkable progress towards the conjecture of Sárközy [17] and showed that the conjecture holds with $\mathcal{A} = \mathcal{B}$. That is, $\mathcal{Q} \neq \mathcal{A} + \mathcal{A}$ for any set $\mathcal{A} \subseteq \mathbb{F}_p$. The method, however, does not seem to extend to other subgroups. Shkredov [18] has also independently observed that $\log p$ can be removed from the bounds (1) and (2) (which is a special case of Theorem 7 below).

We recall that the expressions $A \ll B$, $B \gg A$ and $A = O(B)$ are each equivalent to the statement that $|A| \leq cB$ for some constant c. Throughout the paper, the implied constants in these symbols may depend on the real parameter $\varepsilon > 0$ and the integer parameter $\nu \geq 1$, and are absolute otherwise.

We also use the convention that for elements $\lambda, \mu \in \mathbb{F}_q$ and a set $\mathcal{S} \subseteq \mathbb{F}_q$,

$$\lambda \cdot \mathcal{S} + \mu = \{\lambda s + \mu \ : \ s \in \mathcal{S}\},$$

reserving, say, $2\mathcal{S}$ for

$$2\mathcal{S} = \mathcal{S} + \mathcal{S}.$$

2. Bounds of Multiplicative Character Sums

We refer to [12] for a background on multiplicative characters.

First we recall the Weil bound of multiplicative character sums, see [12, Theorem 11.23].

Lemma 1. *For any polynomial $F(X) \in \mathbb{F}_q[X]$ with D distinct zeros in the algebraic closure of $\mathbb{F}_q$ and which is not a perfect dth and any non-trivial multiplicative character χ of $\mathbb{F}_q^*$ of order d, we have*

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(F(x)\right) \right| \le (D-1)q^{1/2}.$$

We note that the following result is slightly more precise than a bound of Karatsuba [14] (see also [15, Chapter VIII, Problem 9]) that applies to double character sums over arbitrary sets.

Lemma 2. *Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q$ be two arbitrary sets. For any non-trivial multiplicative character χ of $\mathbb{F}_q^*$ and any positive integer ν, we have*

$$\sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(a+b) \ll (\#\mathcal{A})^{(2\nu-1)/2\nu} \left((\#\mathcal{B})^{1/2} q^{1/2\nu} + \#\mathcal{B} q^{1/4\nu} \right).$$

3. A Bound on the Intersection of Shifted Subgroups

Let us consider a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_q^*$. The following bound for $m = 1$ is due to Garcia and Voloch [9], see also [11, 16]. For a fixed $m \ge 1$ it follows instantly from a result of Shkredov and Vyugin [19, Corollary 1.2] by taking $s = 1$, $t = \#\mathcal{G}$, $k = m-1$ and $B = \left\lfloor (\#\mathcal{G})^{1/(2k+1)} \right\rfloor + 1$.

Lemma 3. *Assume that for a fixed integer $m \ge 2$ we have a prime p satisfies:*

$$p \ge 4(m-1)\#\mathcal{G}\left((\#\mathcal{G})^{1/(2m-1)} + 1 \right).$$

Then for pairwise distinct $b_1, \ldots, b_m \in \mathbb{F}_p^*$ the bound

$$\#\left(\bigcap_{i=1}^{m} (\mathcal{G} + b_i) \right) \le 4m\left((\#\mathcal{G})^{1/(2m-1)} + 1 \right)^m$$

holds.

4. A Result from Additive Combinatorics

We extend in a natural way our definition of the sums set $\mathcal{A}+\mathcal{B}$ to other operations on sets. For example, for $\mathcal{A} \subseteq \mathbb{F}_q$ we have

$$\mathcal{A}^2 = \{a_1 a_2 \ : \ a_1, a_2 \in \mathcal{A}\}$$

and

$$\mathcal{A}(\mathcal{A}+1) = \{a_1(a_2+1) \ : \ a_1, a_2 \in \mathcal{A}\}.$$

We also need the following combination of two results of Garaev and Shen [8, Theorems 1 and 2].

Lemma 4. *For any $\varepsilon > 0$ there exists some $\delta > 0$ such that for any prime p and set $\mathcal{A} \subseteq \mathbb{F}_p$ of size $\#\mathcal{A} \le p^{1-\varepsilon}$ we have*

$$\#\left(\mathcal{A}(\mathcal{A}+1)\right) \gg (\#\mathcal{A})^{57/56+o(1)}.$$

We remark that for sets f size $\#\mathcal{A} \le p^{1/2}$ of Jones and Roche-Newton [13], have improved [8, Theorem 1], however this is not essential for our final estimate. Furthermore, for sets with $p^{\varepsilon}\#\mathcal{A} \le p^{1-\varepsilon}$ the estimate of Lemma 4 is also given by Bourgain [3].

5. Preliminary Estimates

Let $\mathcal{G}_d \subseteq \mathbb{F}_q$ be the group of dth powers. We start with the following generalisation of the bound (1), which closely follows the arguments of [6, 17].

Lemma 5. *Let $d \mid q-1$. Then for any nontrivial decomposition of $\mathcal{G}_d$ into some sets $\mathcal{A}$ and $\mathcal{B}$, we have*

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \ge (2+o(1)) \frac{q^{1/2}\log d}{d^2 \log q}$$

as $q \to \infty$.

Proof. Let $K = \#\mathcal{A}$ and $L = \#\mathcal{B}$. Assume that $K \ge L$. Maybe an additive shift by an element of $b \in \mathcal{B}$, that is considering $\mathcal{A}+a$ and $\mathcal{B}-b$ we can assume that $0 \in \mathcal{B}$ and thus $\mathcal{A} \subseteq \mathcal{G}_d$.

First we show that

$$L \ge \left(\frac{1}{\log 2} + o(1)\right) \log(q^{1/2}/d). \tag{5}$$

Indeed, for any $u \in \mathcal{G}_d$ we have

$$u - b \in \mathcal{A} \subseteq \mathcal{G}_d \tag{6}$$

for at least one $b \in \mathcal{B}$. We now show that if (5) does not hold then this is impossible.

Let $\mathcal{X}_d$ be the set of all multiplicative characters of $\mathbb{F}_q^*$ with $\chi^d = \chi_0$ where χ_0 is the principal character. We also define $\mathcal{X}_d^* = \mathcal{X}_d \setminus \{\chi_0\}$. We note that $v \in \mathcal{G}_d$ if and only if

$$\frac{1}{d} \sum_{\chi \in \mathcal{X}_d} \chi(v) = \begin{cases} 1, & \text{if } v \in \mathcal{G}_d, \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, the condition (6) implies

$$\prod_{b \in \mathcal{B}} \left(1 - \frac{1}{d} \sum_{\chi \in \mathcal{X}_d} \chi(u-b)\right) = 0.$$

Since elements of $\mathcal{G}_d$ are all of the form x^d, $x \in \mathbb{F}_q^*$, we see that the sum

$$W = \sum_{x \in \mathbb{F}_q^*} \prod_{b \in \mathcal{B}} \left(1 - \frac{1}{d} \sum_{\chi \in \mathcal{X}_d} \chi(x^d - b)\right)$$

vanishes.

On the other hand, separating the contribution of the principal characters, we write

$$\begin{aligned} W &= \sum_{x \in \mathbb{F}_q^*} \prod_{b \in \mathcal{B}} \left(\frac{d-1}{d} - \frac{1}{d} \sum_{\chi \in \mathcal{X}_d^*} \chi(x^d - b)\right) \\ &= (q-1)\left(\frac{d-1}{d}\right)^L + R, \end{aligned} \tag{7}$$

where, after the change of order of summation we obtain

$$\begin{aligned} R &= \frac{1}{d^L} \sum_{\substack{\mathcal{C} \subseteq \mathcal{B} \\ \mathcal{C} \neq \emptyset}} (-1)^{\#\mathcal{C}} (d-1)^{L - \#\mathcal{C}} \sum_{x \in \mathbb{F}_q^*} \prod_{c \in \mathcal{C}} \sum_{\chi \in \mathcal{X}_d^*} \chi(x^d - c) \\ &= \frac{1}{d^L} \sum_{\ell=1}^{L} (-1)^{\ell} (d-1)^{L-\ell} \sum_{\substack{\mathcal{C} \subseteq \mathcal{B} \\ \#\mathcal{C} = \ell}} \sum_{x \in \mathbb{F}_q^*} \prod_{c \in \mathcal{C}} \sum_{\chi \in \mathcal{X}_d^*} \chi(x^d - c). \end{aligned} \tag{8}$$

For every set $\mathcal{C} = \{c_1, \ldots, c_\ell\}$ of cardinality ℓ, we have

$$\sum_{x \in \mathbb{F}_q^*} \prod_{c \in \mathcal{C}} \sum_{\chi \in \mathcal{X}_d^*} \chi(x^d - c) = \sum_{\chi_1, \ldots, \chi_\ell \in \mathcal{X}_d^*} \sum_{x \in \mathbb{F}_q^*} \prod_{i=1}^{\ell} \chi_i(x^d - c_i). \tag{9}$$

Clearly Lemma 1 applies to the inner sum and yields

$$\left| \sum_{x \in \mathbb{F}_q^*} \prod_{i=1}^{\ell} \chi_i(x^d - c_i) \right| < d\ell q^{1/2}.$$

Hence

$$\left| \sum_{\chi_1,\ldots,\chi_\ell \in \mathcal{X}_d^*} \sum_{x\in\mathbb{F}_q^*} \prod_{i=1}^{\ell} \chi_i(x^d - c_i) \right| < d(d-1)^\ell \ell q^{1/2}.$$

Thus, substituting this bound in (9), and then the resulting estimate in (8), we obtain

$$R < dq^{1/2} \left(\frac{d-1}{d}\right)^L \sum_{\ell=1}^{L} \binom{L}{\ell} \ell = dL2^{L-1} \left(\frac{d-1}{d}\right)^L q^{1/2}.$$

Recalling (7), we derive

$$\left| W - (q-1)\left(\frac{d-1}{d}\right)^L \right| < dL2^{L-1} \left(\frac{d-1}{d}\right)^L q^{1/2}.$$

Therefore, if $W = 0$ then $q - 1 < dL2^{L-1}q^{1/2}$ and (5) follows.

For $d = 2$ the result follows from a direct generalisation of (1) to arbitrary finite fields.

We now assume that $d \geq 3$, as otherwise there is nothing to prove and set

$$L^* = \left\lceil \frac{\log(q^{1/2}/d)}{\log d} \right\rceil .$$

Next, we choose an arbitrary subset $\mathcal{B}^* \subseteq \mathcal{B}$ of cardinality L^* (which by (5) is possible for a sufficiently large p).

We denote by N is the number of $u \in \mathcal{G}_d$ satisfying (6) for every $b \in \mathcal{B}^*$. Clearly $N \geq K$. On the other hand, as before, we write

$$\begin{aligned} N &= \sum_{u\in\mathcal{G}_d} \prod_{b\in\mathcal{B}^*} \left(\frac{1}{d} \sum_{\chi\in\mathcal{X}_d} \chi(u-b) \right) = \frac{1}{d} \sum_{x\in\mathbb{F}_q^*} \prod_{b\in\mathcal{B}^*} \left(\frac{1}{d} \sum_{\chi\in\mathcal{X}_d} \chi(x^d - b) \right) \\ &= \frac{1}{d^{L^*+1}} \sum_{x\in\mathbb{F}_q^*} \prod_{b\in\mathcal{B}^*} \sum_{\chi\in\mathcal{X}_d} \chi(x^d - b). \end{aligned}$$

Exactly the same argument as in the previous estimation of W implies

$$\begin{aligned} \left| N - \frac{(q-1)}{d^{L^*+1}} \right| &\leq \frac{1}{d^{L+1}} \left| \sum_{x\in\mathbb{F}_q^*} \prod_{b\in\mathcal{B}^*} \sum_{\chi\in\mathcal{X}_d^*} \chi(x^d - b) \right| \\ &= \frac{dq^{1/2}}{d^{L^*+1}} \sum_{\substack{\mathcal{C}\subseteq\mathcal{B}^* \\ \mathcal{C}\neq\emptyset}} (d-1)^{\#\mathcal{C}} \#\mathcal{C} = \frac{q^{1/2}}{d^{L^*}} \sum_{\ell=1}^{L^*} \binom{L^*}{\ell} (d-1)^\ell \ell \\ &= \frac{q^{1/2}}{d^{L^*}} L^* d^{L^*-1}(d-1) < L^* q^{1/2}. \end{aligned}$$

Recalling the choice of L^* we immediately derive

$$K \le N \le \left(\frac{1}{2} + o(1)\right) \frac{dq^{1/2}\log q}{\log d}. \tag{10}$$

Since we obviously have $KL \ge \#\mathcal{G}_e = (q-1)/d$ the result follows. □

We now use Lemma 4 to study nontrivial additive decompositions of small subgroups.

Lemma 6. *For any $\varepsilon > 0$ there exists some $\kappa > 0$ such that if for a prime $q = p$ and a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order $\#\mathcal{G} < p^{1-\varepsilon}$ there is a nontrivial decomposition into some sets $\mathcal{A}$ and $\mathcal{B}$, then*

$$(\#\mathcal{G})^{\kappa} \le \min\{\#\mathcal{A}, \#\mathcal{B}\} \le \max\{\#\mathcal{A}, \#\mathcal{B}\} \ll (\#\mathcal{G})^{1-\kappa}.$$

Proof. Assume that $\#\mathcal{A} \ge \#\mathcal{B}$. Also, as in the proof of Lemma 5, we see that we can assume that $\#\mathcal{A} \subseteq \mathcal{G}$.

Since $\#\mathcal{B} \ge 2$, there is $b \in \mathcal{B}$ with $b \ne 0$. Then, from the identity

$$\mathcal{A}(\mathcal{A} + b) = b^2(b^{-1}\mathcal{A})(b^{-1}\mathcal{A} + 1)$$

and Lemma 4 we see that $\#\left(\mathcal{A}(\mathcal{A}+b)\right) \ge (\#\mathcal{A})^{1+\delta}$ for some $\delta > 0$ that depends only on ε. On the other hand, we obviously have $\mathcal{A}(\mathcal{A}+b) \subseteq \mathcal{G}$, thus $\#\mathcal{A} \le (\#\mathcal{G})^{1/(1+\delta)}$. Since $\#\mathcal{A}\#\mathcal{B} \ge \#\mathcal{G}$, the result now follows. □

6. Decompositions of Large Multiplicative Subgroups and the Set of Primitive Roots

Clearly the bound (10) is of the same order of magnitude as (2). Here we use Lemma 2 to generalise and improve (2) and (4).

Theorem 7. *For any $\varepsilon > 0$, if for a subgroups $\mathcal{G} \subseteq \mathbb{F}_q^*$ of order $\#\mathcal{G} \ge q^{3/4+\varepsilon}$ or the set of primitive roots $\mathcal{R} \subseteq \mathbb{F}_q^*$ there is a nontrivial decomposition into some sets $\mathcal{A}$ and $\mathcal{B}$, then*

$$\max\{\#\mathcal{A}, \#\mathcal{B}\} \ll q^{1/2}.$$

Proof. Clearly, if $\mathcal{R} = \mathcal{A} + \mathcal{B}$ is a decomposition of the set of primitive roots, then multiplying each elements of $\mathcal{A}$ and $\mathcal{B}$ by a fixed quadratic non-residue ξ we obtain

$$\xi \cdot \mathcal{A} + \xi \cdot \mathcal{B} \subseteq \mathcal{Q}.$$

Let $d = (q-1)/\#\mathcal{G}$, thus $\mathcal{G} = \mathcal{G}_d$ in the notation of Section 5.

We also remark that $d \ll q^{1/4-\varepsilon}$, so by Lemma 5 we have

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \ge q^{\varepsilon} \tag{11}$$

for any nontrivial decomposition of $\mathcal{G}_d$. Furthermore, one can check that the bound (3) can be extended to arbitrary finite fields, so (11) also holds for the sets in any nontrivial decomposition of $\mathcal{R}$.

Thus, it is enough to show that any sets $\mathcal{A}$ and $\mathcal{B}$ with (11) such that $\mathcal{A}+\mathcal{B} \subseteq \mathcal{G}_d$ we have

$$\max\{\#\mathcal{A}, \#\mathcal{B}\} \ll q^{1/2}. \tag{12}$$

Assume that $\#\mathcal{A} \ge \#\mathcal{B}$.

Now, let $\chi \in \mathcal{X}_d^*$ be any non-principal character of $\mathbb{F}_q^*$. If $\mathcal{A}+\mathcal{B} \subseteq \mathcal{G}_d$ then we have

$$\sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \chi(a+b) = \#\mathcal{A}\#\mathcal{B}.$$

Comparing this with the bound of Lemma 2, we derive

$$\#\mathcal{A}\#\mathcal{B} \ll (\#\mathcal{A})^{(2\nu-1)/2\nu} \left((\#\mathcal{B})^{1/2} q^{1/2\nu} + \#\mathcal{B} q^{1/4\nu}\right). \tag{13}$$

Taking $\nu = \lceil \varepsilon^{-1} \rceil$, we see that the condition (11) implies

$$(\#\mathcal{B})^{1/2} q^{1/2\nu} \le \#\mathcal{B} q^{1/4\nu}.$$

Hence (13) can now be re-written as

$$\#\mathcal{A}\#\mathcal{B} \ll (\#\mathcal{A})^{(2\nu-1)/2\nu} \#\mathcal{B} q^{1/4\nu},$$

which implies (12), and concludes the proof. $\square$

Obviously, if $\mathcal{G} = \mathcal{A}+\mathcal{B}$ then $\#\mathcal{G} \le \#\mathcal{A}\#\mathcal{B}$. Hence Theorem 7 implies that any nontrivial decomposition of a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ of order $\#\mathcal{G} \ge q^{3/4+\varepsilon}$ into some sets $\mathcal{A}$ and $\mathcal{B}$, we have

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \gg \#\mathcal{G} q^{-1/2}$$

that is stronger than Lemma 5 and for $\mathcal{G} = \mathcal{Q}$ improves the bound (2) of Sárközy [17].

Similarly, any nontrivial decomposition of $\mathcal{R}$ into some sets $\mathcal{A}$ and $\mathcal{B}$, we have

$$\min\{\#\mathcal{A}, \#\mathcal{B}\} \gg \#\mathcal{R} q^{-1/2} = \varphi(q-1) q^{-1/2},$$

that improves the bound (4) of Dartyge and Sárközy [6].

7. Decompositions of Small Multiplicative Subgroups

We now use Lemma 4 to study nontrivial additive decompositions of small subgroups of prime fields that is, subgroups $\mathcal{G} \subseteq \mathbb{F}_p^*$ with a prime p of cardinality $\#\mathcal{G}$ to which the bound of Theorem 7 is either weak or does not apply (for example for subgroups of order $\#\mathcal{G} < p^{3/4}$).

Theorem 8. *Let $q = p$ be prime. If for a subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ there is a nontrivial decomposition into some sets $\mathcal{A}$ and $\mathcal{B}$, then*

$$(\#\mathcal{G})^{1/2+o(1)} = \min\{\#\mathcal{A}, \#\mathcal{B}\} \le \max\{\#\mathcal{A}, \#\mathcal{B}\} = (\#\mathcal{G})^{1/2+o(1)},$$

as $\#\mathcal{G} \to \infty$.

Proof. Assume that $\#\mathcal{A} \ge \#\mathcal{B}$.

Since $\#\mathcal{A}\#\mathcal{B} \ge \#\mathcal{G}$ it suffices to only establish the upper bound. In particular, it is enough to show that for an arbitrary $\eta > 0$ we have

$$\#\mathcal{A} \le (\#\mathcal{G})^{1/2+\eta}. \tag{14}$$

Let us fix some sufficiently small $\eta > 0$. In particular, we assume that that $\eta < 1/6$, thus $1/(1+2\eta) > 3/4$. Then for $\#\mathcal{G} \ge p^{1/(1+2\eta)}$ the bound (14) follows from Theorem 7.

So we now assume that $\#\mathcal{G} < p^{1/(1+2\eta)}$. Then clearly for any $m \ge 2$ and a sufficiently large p the condition of Lemma 3 is satisfied.

By Lemma 6, the set $\#\mathcal{B}$ is large enough, so that it has m distinct elements $b_1, \ldots, b_m$. We now observe that for every $i = 1, \ldots, m$ we have $\mathcal{A} \subseteq \mathcal{G} - b_i$. Thus taking m sufficiently large we see that Lemma 3 implies (14). Since $\#\mathcal{A}\#\mathcal{B} \ge \#\mathcal{G}$, the result now follows. □

Clearly one can choose m as a growing function of $\#\mathcal{G}$ and get more explicit bounds in Theorem 8.

8. Comments

We remarks that it is natural to try to obtain analogues of our results for the dual problem of nontrivial multiplicative decompositions of intervals in $\mathbb{F}_p$. That is, one can consider representations $\mathcal{I} = \mathcal{A}\mathcal{B}$ of sets $\mathcal{I} = \{m+1, \ldots, m+n\} \subseteq \mathbb{F}_p$ of n consecutive residues modulo p with two arbitrary sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p^*$ such that $\#\mathcal{A} \ge \#\mathcal{B} \ge 2$. Certainly various conjectures, similar to those of [6, 17], can be about the non-existence of such decompositions. Here we merely show that some of the above methods apply to multiplicative decompositions too. For example, by a result of Bourgain [4], for any two sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$ with $\mathcal{A}, \mathcal{B} \ne \{0\}$, we have

$$\#\left(8\mathcal{A}\mathcal{B} - 8\mathcal{A}\mathcal{B}\right) > \frac{1}{2} \min\left\{\#\mathcal{A}\#\mathcal{B}, p-1\right\}.$$

On the other hand, if $\mathcal{A}\mathcal{B} = \mathcal{I}$ then

$$\#\left(8\mathcal{A}\mathcal{B} - 8\mathcal{A}\mathcal{B}\right) \le 16\#\mathcal{I}.$$

Thus for $\#\mathcal{I} < (p-1)/32$ we derive very tight bounds:

$$\#\mathcal{I} \le \#\mathcal{A}\#\mathcal{B} \le 32\#\mathcal{I}.$$

Now we note, as in the above we can assume that $1 \in \mathcal{B}$, so $\mathcal{A} \subseteq \mathcal{I}$. Using the orthogonality of the exponential function

$$\mathbf{e}_p(z) = \exp(2\pi i z/p)$$

we can write the number of solutions J to the congruence

$$u \equiv ab \pmod p, \qquad u \in \mathcal{I},\ a \in \mathcal{A},\ b \in \mathcal{B},$$

as

$$J = \sum_{u\in\mathcal{I}} \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \frac{1}{p} \sum_{-(p-1)/2 \le \lambda \le (p-1)/2} \mathbf{e}_p(\lambda(u-ab)).$$

Changing the order of summation and separating the contribution $\#\mathcal{A}\#\mathcal{B}\#\mathcal{I}/p$ of terms corresponding to $\lambda = 0$, we obtain

$$\left| J - \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{I}}{p} \right| \le \frac{1}{p} \sum_{1\le|\lambda|\le(p-1)/2} \left| \sum_{u\in\mathcal{I}} \mathbf{e}_p(\lambda u) \right| \left| \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \mathbf{e}_p(\lambda ab) \right|.$$

Using the classical estimate

$$\left| \sum_{a\in\mathcal{A}} \sum_{b\in\mathcal{B}} \mathbf{e}_p(\lambda ab) \right| \le (p\#\mathcal{A}\#\mathcal{B})^{1/2},$$

see, for example, see [5, Equation (1.4)] or [7, Lemma 4.1], together with the bound

$$\left| \sum_{u\in\mathcal{I}} \mathbf{e}_p(\lambda u) \right| \le \frac{p}{|\lambda|},$$

that holds for $1 \le |\lambda| \le (p-1)/2$ see [12, Bound (8.6)]. We derive

$$J - \frac{\#\mathcal{A}\#\mathcal{B}\#\mathcal{I}}{p} \ll (p\#\mathcal{A}\#\mathcal{B})^{1/2} \log p.$$

On the other hand, since $\mathcal{I} = \mathcal{A}\mathcal{B}$ is multiplicative decomposition of $\mathcal{I}$, we have $J = \#\mathcal{A}\#\mathcal{B}$. Thus for any fixed $\varepsilon > 0$, if $\#\mathcal{I} < (1-\varepsilon)p$ then

$$\#\mathcal{A}\#\mathcal{B} \ll p(\log p)^2.$$

One can also consider more general questions about sets of the form

$$F(\mathcal{A},\mathcal{B}) = \{F(a,b)\ :\ a \in \mathcal{A},\ b \in \mathcal{B}\}$$

with $F(X,Y) = \mathbb{F}_q[X,Y]$, representing subgroups and intervals.

Finally, we note that Gyarmati, Konyagin and Sárközy [10] have studied additive decompositions of large subsets (of size close to p) of prime fields $\mathbb{F}_p$. The Weil bound of multiplicative character sums also plays a prominent role in the arguments of [10]. Several more results about decompositions of arbitrary sets can be found in [1, 2].

9. Acknowledgment

The author is grateful to Cecile Dartyge for a careful reading of the manuscript and many valuable comments, to Sergei Konyagin for his suggestion to use the result of Shkredov and Vyugin [19] in the proof of Theorem 8 and to Ilya Shkredov for useful discussions and providing a preliminary version of [18].

This work was supported in part by the ARC Grant DP130100237.

References

[1] N. Alon, 'Large sets in finite fields are sumsets', *J. Number Theory*, **126** (2007), 110–118.

[2] N. Alon, A. Granville and A. Ubis, The number of sumsets in a finite field', *Bull. London Math. Soc.*, **42** (2010), 784–794.

[3] J. Bourgain, 'More on the sum-product phenomenon in prime fields and its applications', *Int. J. Number Theory*, **1** (2005), 1–32.

[4] J. Bourgain, 'Multilinear exponential sums in prime fields under optimal entropy condition on the sources', *Geom. and Func. Anal.*, **18** (2009), 1477–1502.

[5] J. Bourgain and M. Z. Garaev, 'On a variant of sum-product estimates and explicit exponential sum bounds in prime fields', *Math. Proc. Cambr. Phil. Soc.*, **146** (2008), 1–21.

[6] C. Dartyge and A. Sárközy, 'On additive decompositions of the set of primitive roots modulo p', *Monat. Math.*, (to appear).

[7] M. Z. Garaev, 'Sums and products of sets and estimates of rational trigonometric sums in fields of prime order', *Russian Math. Surveys*, **65** (2010), 599–658 (Transl. from *Uspekhi Mat. Nauk*).

[8] M. Z. Garaev and C.-Y. Shen, 'On the size of the set $A(A+1)$', *Math. Zeit.*, **265** (2010), 125–132.

[9] A. Garcia and J. F. Voloch, 'Fermat curves over finite fields', *J. Number Theory*, **30**(1988), 345–356.

[10] K. Gyarmati, S. V. Konyagin and A. Sárközy, 'On the reducibility of large sets of residues modulo p', *Preprint*, 2012.

[11] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum', *Ouart. J. Math.*, **51** (2000), 221–235.

[12] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[13] T. G. F. Jones and O. Roche-Newton, 'Improved lower bound on the set $A(A+1)$', *J. Combin. Theory*, **120** (2013), 515–526.

[14] A. A. Karatsuba, 'The distribution of values of Dirichlet characters on additive sequences', *Doklady Acad. Sci. USSR*, **319** (1991), 543–545 (in Russian).

[15] A. A. Karatsuba, *Basic analytic number theory*, Springer-Verlag, 1993.

[16] S. V. Konyagin, 'Bounds of exponential sums over subgroups and Gauss sums', *Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications*, Moscow Lomonosov State Univ., Moscow, 2002, 86–114 (in Russian).

[17] A. Sárközy, 'On additive decompositions of the set of the quadratic residues modulo p', *Acta Arith.*, (to appear).

[18] I. D. Shkredov, 'Sumsets in quadratic residues', *Preprint*, 2013.

[19] I. V. Vyugin and I. D. Shkredov, 'On additive shifts of multiplicative subgroups', *Sbornik: Mathematics*, **203** (2012), 844–863 (Transl. from Sbornik: Mathematics)

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: igor.shparlinski@mq.edu.au